AMENDMENTS TO THE CLAIMS:

Please amend Claims 1, 3, 4, 8, 11, 16 -18, and 20 as follows.

Please add new Claims 38 and 39.

1. (Currently Amended) An information processing apparatus for embedding authentication information into digital information, comprising:

generating means for generating authentication information on the basis of the digital information;

~~acquisition means for acquiring information from the authentication information and the digital information;~~

~~embedding~~ digital watermarking means for embedding the generated authentication information into the digital information ~~as a digital watermark, on the basis of information acquired by said acquisition means; and~~ by adding a value to or subtracting a value from each of plural elements which form the digital information;

~~output means for outputting information acquired by said acquisition means~~

wherein, if after the addition or subtraction an element has a value exceeding a variable range permitted for the element, said digital watermarking means excludes the element from an embedding process upon embedding the generated authentication information into the digital information.

2. (Original) The apparatus according to claim 1, wherein the authentication information is a digital signature.

3. (Currently Amended) The apparatus according to claim [[1]] 2, further comprising encryption means for encrypting the digital information using a secret key, and wherein the digital signature is data obtained by encrypting the digital information using the secret key.

4. (Currently Amended) The apparatus according to claim [[1]] 2, further comprising Hash value calculation means for calculating a Hash value of the digital information, and encryption means for encrypting the Hash value using a secret key, and wherein the digital signature is data obtained by encrypting the Hash value of the digital information using the secret key.

5. (Original) The apparatus according to claim 1, wherein the authentication information is MAC.

6. (Original) The apparatus according to claim 5, further comprising Hash value calculation means for calculating a Hash value of the digital information, and arithmetic operation means for arithmetically operating the Hash value using a secret key, and wherein the MAC is data obtained by arithmetically operating the Hash value of the digital information using the secret key.

7. (Original) The apparatus according to claim 2, wherein the authentication information includes at least one of date information, position information, time

information, unique information of an apparatus, and unique information of a person who signed, in addition to the digital signature.

8. (Currently Amended) An information processing apparatus for authenticating digital information in which authentication information is embedded as a digital watermark ~~on the basis of information acquired from the authentication information and the digital information~~ by adding a value to or subtracting a value from each of plural elements which form the digital information, wherein elements having a value exceeding a variable range permitted for the element after the addition or subtraction are excluded from an embedding process upon embedding the authentication information into the digital information, comprising:

means for inputting information identifying elements excluded from the embedding process;

means for extracting, as first authentication information, the authentication information embedded as the digital watermark from the digital information, on the basis of the acquired information identifying elements excluded from the embedding process;

digital watermark removal means for removing the extracted authentication information from the digital information as the digital watermark, and restoring tentative original digital information;

generation means for generating second authentication information on the basis of the tentative original digital information restored by removing the digital watermark by said digital watermark removal means; and

comparison means for comparing the first authentication information with second authentication information.

9. (Original) The apparatus according to claim 8, further comprising informing means for, when the first authentication information and second authentication information are equal to each other, informing that the input digital information has not been tampered with, and for, when the first authentication information and second authentication information are not equal to each other, informing that the input digital information has been tampered with.

10. (Original) The apparatus according to claim 8, wherein the authentication information is a digital signature.

11. (Currently Amended) The apparatus according to claim [[8]] 10, further comprising decryption means for decrypting the digital signature using a public key, and wherein said comparison means compares information obtained by decrypting the ~~second~~ first authentication information with the ~~first~~ second authentication information.

12. (Original) The apparatus according to claim 8, further comprising Hash value calculation means for calculating a Hash value of the digital information from which the digital watermark has been removed, and decryption means for decrypting the digital signature using a public key, and wherein said comparison means compares information

obtained by decrypting the second authentication information using the public key, with the Hash value.

13. (Original) The apparatus according to claim 8, wherein the authentication information is MAC.

14. (Original) The apparatus according to claim 12, further comprising Hash value calculation means for calculating a Hash value of the digital information from which the digital watermark has been removed, and arithmetic operation means for arithmetically operating the MAC using a secret key, and wherein said comparison means compares information obtained by decrypting the MAC using the secret key with the Hash value.

15. (Original) The apparatus according to claim 8, wherein the authentication information includes at least one of date information, position information, time information, unique information of an apparatus, and unique information of a person who signed, in addition to the digital signature.

16. (Currently Amended) A method of controlling an information processing apparatus for embedding authentication information into digital information, comprising:

a step of generating authentication information on the basis of the digital information;

~~a step of acquiring information from the authentication information and the digital information;~~

a digital watermarking step of embedding the generated authentication information into the digital information ~~as a digital watermark, on the basis of information acquired by said acquiring step; and~~ by adding a value to or subtracting a value from each of plural elements which form the digital information;

~~a step of outputting information acquired by said acquiring step~~

wherein, if after the addition or subtraction an element has a value exceeding a variable range permitted for the element, said digital watermarking step excludes the element from an embedding process upon embedding the generated authentication information into the digital information.

17. (Currently Amended) A method of controlling an information processing apparatus for authenticating digital information in which authentication information is embedded as a digital watermark ~~on the basis of information acquired from the authentication information and the digital information~~ by adding a value to or subtracting a value from each of plural elements which form the digital information, wherein elements having a value exceeding a variable range permitted for the element after the addition or subtraction are excluded from an embedding process upon embedding the authentication information into the digital information, comprising:

the step of inputting information identifying elements excluded from the embedding process;

the step of extracting, as first authentication information, the authentication information embedded as the digital watermark from the digital information on the basis of the acquired information identifying elements excluded from the embedding process;

the digital watermark removal step of removing the extracted authentication information from the digital information as the digital watermark, and restoring tentative original digital information;

the generation step of generating second authentication information on the basis of the tentative original digital information restored by removing the digital watermark in the digital watermark removal step; and

the comparison step of comparing the first authentication information with second authentication information.

18. (Currently Amended) A computer program stored in a computer-readable storage medium, which is loaded and executed by a computer to make the computer function as an information processing apparatus for embedding authentication information into digital information, comprising:

a program code of the step of generating authentication information on the basis of the digital information;

~~a program code of the step of acquiring information from the authentication information and the digital information;~~

a program code of the digital watermarking step of embedding the generated authentication information into the digital information ~~as a digital watermark, on the basis of information acquired by said acquiring step; and~~ by adding a value to or subtracting a value from each of plural elements which form the digital information;

~~a program code of the step of outputting information acquired by said acquiring step~~

wherein, if after the addition or subtraction an element has a value exceeding a variable range permitted for the element, said digital watermarking step excludes the element from an embedding process upon embedding the generated authentication information into the digital information.

19. (Previously Presented) A storage medium storing a computer program recited in claim 18.

20. (Currently Amended) A computer program stored in a computer-readable storage medium, which is loaded and executed by a computer to make the computer function as an information processing apparatus for authenticating digital information in which authentication information is embedded as a digital watermark by adding a value to or subtracting a value from each of plural elements which form the digital information, wherein elements having a value exceeding a variable range permitted for the element after the addition or subtraction are excluded from an embedding process upon embedding the authentication information into the digital information, comprising:

a program code of the step of inputting information identifying elements excluded from the embedding process;

a program code of the step of extracting, as first authentication information, the authentication information embedded as the digital watermark from the digital information, on the basis of the acquired information identifying elements excluded from the embedding process;

a program code of the digital watermark removal step of removing the extracted authentication information from the digital information as the digital watermark, and restoring tentative original digital information;

a program code of the generation step of generating second authentication information on the basis of the tentative original digital information restored by removing the digital watermark in the digital watermark removal step; and

a program code of the comparison step of comparing the first authentication information with second authentication information.

21. (Previously Presented) A storage medium storing a computer program recited in claim 20.

22. (Withdrawn) An information embedding apparatus for embedding additional information into elements which form digital data by adding/subtracting a value to/from the elements, comprising:

detection means for detecting an element which has a value that exceeds a range the element can assume after addition/subtraction;

generation means for generating actual embedding information by combining the additional information and information detected by said detection means; and

embedding means for excluding the element which exceeds the range the element can assume after addition/subtraction from an embedding process upon embedding into the digital data, and embedding the actual embedding information generated by said

generation means into the elements, which fall within the range the element can assume, as a digital watermark.

23. (Withdrawn) The apparatus according to claim 22, wherein the digital data is image data, and

said detection means detects a pixel position where a pixel value exceeds a range the pixel value can assume after addition/subtraction.

24. (Withdrawn) The apparatus according to claim 22, further comprising encoding means for compression-encoding at least one of the additional information and the information detected by said detection means, and wherein said generation means generates the actual embedding information on the basis of an encoding result of said encoding means.

25. (Withdrawn) The apparatus according to claim 22, further comprising encryption means for encrypting at least one of the additional information and the information detected by said detection means, and wherein said generation means generates the actual embedding information on the basis of an encryption result of said encryption means.

26. (Withdrawn) The apparatus according to claim 22, further comprising encoding means for converting at least one of the additional information and the information detected by said detection means into an error correction code, and wherein

said generation means generates the actual embedding information on the basis of a conversion result of said encoding means.

27. (Withdrawn) The apparatus according to claim 22, further comprising correction means for correcting the digital data to reduce the number of elements, which have values that exceed the range the element can assume after addition/subtraction, in the digital data, and

wherein said generation means generates the actual embedding information by embedding information indicating correction contents of said correction means.

28. (Withdrawn) An information restoration apparatus for receiving digital data in which information is embedded by an information embedding apparatus recited in claim 22, and restoring original digital data, comprising:

digital watermark extraction means for extracting information embedded into the input digital data; and

digital watermark removal means for removing the embedded information, from the elements which have undergone an embedding process, on the basis of information which specifies elements excluded from the embedding process, and restoring original digital data.

29. (Withdrawn) The apparatus according to claim 28, further comprising decoding means for expanding and decoding at least one of the additional information

extracted by said digital watermark extraction means, the information indicating the elements excluded from the embedding process, and

wherein said digital watermark removal means removes a digital watermark on the basis of a result decoded by said decoding means.

30. (Withdrawn) The apparatus according to claim 28, further comprising decoding means for decrypting and decoding at least one of the additional information extracted by said digital watermark extraction means, the information indicating the elements excluded from the embedding process, and

wherein said digital watermark removal means removes a digital watermark on the basis of a result decoded by said decoding means.

31. (Withdrawn) The apparatus according to claim 28, further comprising decoding means for decoding an error correction code of at least one of the additional information extracted by said digital watermark extraction means, the information indicating the elements excluded from the embedding process, and

wherein said digital watermark removal means removes a digital watermark on the basis of a result decoded by said decoding means.

32. (Withdrawn) A method of controlling an information embedding apparatus for embedding additional information into elements which form digital data by adding/subtracting a value to/from the elements, comprising:

the detection step of detecting an element which has a value that exceeds a range the element can assume after addition/subtraction;

the generation step of generating actual embedding information by combining the additional information and information detected in the detection step; and

the embedding step of excluding the element which exceeds the range the element can assume after addition/subtraction from an embedding process upon embedding into the digital data, and embedding the actual embedding information generated in the generation step in the elements, which fall within the range the element can assume, as a digital watermark.

33. (Withdrawn) A method of controlling an information restoration apparatus for receiving digital data in which information is embedded by an information embedding apparatus recited in claim 22, and restoring original digital data, comprising:

the digital watermark extraction step of extracting information embedded into the input digital data; and

the digital watermark removal step of removing the embedded information, from the elements which have undergone an embedding process, on the basis of information which specifies elements excluded from the embedding process, and restoring original digital data.

34. (Withdrawn) A computer program which is loaded and executed by a computer to make the computer function as an information embedding apparatus for

embedding additional information into elements which form digital data by adding/subtracting a value to/from the elements, comprising:

a program code of the detection step of detecting an element which has a value that exceeds a range the element can assume after addition/subtraction;

a program code of the generation step of generating actual embedding information by combining the additional information and information detected in the detection step; and

a program code of the embedding step of excluding the element which exceeds the range the element can assume after addition/subtraction from an embedding process upon embedding into the digital data, and embedding the actual embedding information generated in the generation step into the elements, which fall within the range the element can assume, as a digital watermark.

35. (Withdrawn) A computer program which is loaded and executed by a computer to make the computer function as an information restoration apparatus for receiving digital data in which information is embedded by an information embedding apparatus recited in claim 22, and restoring original digital data, comprising:

a program code of the digital watermark extraction step of extracting information embedded into the input digital data; and

a program code of the digital watermark removal step of removing the embedded information, from the elements which have undergone an embedding process, on the basis of information which specifies elements excluded from the embedding process, and restoring original digital data.

36. (Withdrawn) A storage medium storing a computer program recited in claim 34.

37. (Withdrawn) A storage medium storing a computer program recited in claim 35.

38. (New) The apparatus according to claim 1, further comprising output means for outputting information identifying elements excluded from the embedding process.

39. (New) The method according to claim 16, further comprising the output step of outputting information identifying elements excluded from the embedding process.